MATH 314 Spring 2018 - Class Notes

1/31/2019

Scribe: Kyle Roberts

Summary: The first real crypto-cipher being the Caesar or shift cipher. How to encrypt a message using modular arithmetic with an encryption function and how to decrypt using a decryption function. Plan of attacks against the Caesar cipher and how to make the encryption stronger.

Notes: Caesar cipher or shift cipher

- Shift alphabet to the right using a key (in this case, a number 0-25)
- Map letters to numbers to mathematically represent them (a:0, b:1, ... z:25)
- Encryption Function: $E(x) -> x + K \pmod{26}$ (Where K is the key or shift)
- Key is how much to shift the alphabet
- We say that a and b are equivalent modulo m where: $a \equiv b \pmod{m}$ if they have the same remainder when divided by m (Or a - b is divisible by m)

Example:

K = 7

Encrypt the plain text "bat"

b:1, a:0, t:19

$$E(1) -> 1 + 7 \equiv 8 \pmod{26} -> I$$

$$E(0) -> 0 + 7 \equiv 7 \pmod{26} -> H$$

$$E(19) -> 19 + 7 \equiv 26 \pmod{26} \equiv 0 \pmod{26} -> A$$

Encrypted text is `"IHA"` How to decrypt:

$$D(x) = x - k \pmod{26}$$

$$D(8) = 8 - 7 \equiv 1 \pmod{26}$$

$$D(7) = 7 - 7 \equiv 0 \pmod{26}$$

$$D(0) = 0 - 7 \equiv -7 \pmod{26} \equiv 19 \pmod{26}$$

The resulting number maps to the mapped letter of the alphabet

- Alice encrypts plain text to `cipher text`. Eve is eavesdropping and can read the `cipher text`. Bob receives the `cipher text` and uses the key to decrypt to plain text.
- **Kerchoff's Principle**: When analyzing the security of a cipher - one should assume the attacker knows everything about the system except for the key being used.
- The three types of attacks against cryptosystems are:
    1. Cipher text only: Attacker only has access to encrypted messages and wants to recover the key
    2. Known plain text attacks: Attacker knows a plain text message as well as its cipher text and wants to recover the key
    3. Chosen plain text attack: Attacker gets a copy of the encryption machine and encrypts any plain text he/she wants and finds out what the cipher text is and therefore knows the key

These attacks against the Caesar cipher:

1. Cipher text only:
    - Brute force: Try all 26 possible keys and look for the messages that carry information
    - Frequency attack: Use the frequency of letters in the plain text to make an educated guess, but is only useful if there is a lot of letters
2. Known plain text attack: Knows "n" maps to `"Y"`

$$n -> 13\texttt{Y} -> 24$$

$$E(13) = 13 + K \pmod{26}$$

$$K = 24 - 13 = 11$$

   Key is 11, so shift the alphabet 11 letters to the right.
3. Chosen plain text: Choose "a", whichever it encrypts to, use the equation above to get the key

How to make the Caesar cipher harder to decrypt:

- Need to increase number of keys
- Consider multiplication in modular arithmetic

$$a * b \pmod{26}$$

- Sometimes we can do division (Though we might have more than one answer)